Attorney Docket Ref.: 41051.P010
Client Ref: GW10.116

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

Avoiding Attachment Of Ineligible Smart Interchangeable Cover To An Electronic Device

Inventor(s):
Peter Zatloukal
Eric Engstrom
Paul R. Nash
David Pike

Prepared by:
COLUMBIA IP LAW GROUP, PC

Express Mail Label No.: EV051081564US
Date of Deposit: November 30, 2001

Avoiding Attachment Of An Ineligible Smart Interchangeable Cover To An Electronic Device

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of counterfeit avoidance techniques. More specifically, the present invention relates to the avoidance of attachment of an ineligible (such as, counterfeit) smart interchangeable cover to a base portion of an electronic apparatus (to personalize or functionally enrich the electronic apparatus).

2. Background Information

With the proliferation of electronic devices, especially mobile electronic devices, such as, mobile phones, hand-held personal computers, and so forth, these devices have gained the status of personal appliances to a person. As a result, increasingly, users desire to personalize these devices. For example, in addition to a wide variety of body casing colors, interchangeable faceplates of various colors and artistic designs are available for a variety of mobile phones to allow the users to have even greater choices providing different physical appearances to their own devices. Additionally, a variety of non-standard features such as games, screen-savers and ring tones can be downloaded from various websites into the devices to further personalize the devices. Similarly, hand-held personal computers and personal digital assistants also come in various colors, with various applications software, screen savers and wallpapers. In this document, the terms "personalization feature" or "feature" are used interchangably to refer to these

types of software programs and/or data and the effects they may have on the appearance or functionality of a device. In this definition, items such as games, screensavers or ringtones are illustrative and not the exclusive types of features that may be included in the meaning of "personalization feature."

These approaches to personalization suffer from a number of disadvantages. First, they are disjoint. Typically, a user may go to a mall or an online e-commerce site to shop and purchase, e.g. a faceplate with design and/or color that is of interest to the user. Then, the user may go online to websites to search and look for a custom ring tone or a screen saver of interest to the user. It is the user's responsibility to choose and combine the appropriate hardware, i.e. faceplate design/color, with the software behavior, i.e. custom ring tone etc. to create a total personality. The process is cumbersome for many users, especially for the more novice users, as the proliferation of mobile electronic devices reaches more and more users. Moreover, the approaches do not facilitate quick and timely changes to the personality to be taken on by the mobile electronic devices. These shortcomings apply equally to personalization of other electronic devices, such as game consoles.

In co-pending U.S. Provisional Application No. 60/306,326, titled "Personalizing Electronic Devices and Smart Covering", filed on July 17, 2001, various methods and apparatus for personalizing or field enhancing the functionalities of electronic devices are disclosed. While these methods and apparatus brought forth numerous benefits and advantages, they also give rise to a need to prevent ineligible (such as counterfeit) smart interchangeable covers from being inappropriately employed.

Thus, methods and apparatuses that can secure and avoid attachment of ineligible (such as counterfeit) smart interchangeable covers to electronic devices

are desired. As those skilled in the art would appreciate, sophisticated security measures are costly to implement. Moreover, theoretically, even the most sophiscated commercial security measures may be compromised, given sufficient resource and time. Thus, it is further desired that the security and avoidance method provides a sercurity versus cost tradeoff that is commensurate to both the security needs and the economics of the electronic apparatuses on which the methods are practiced.

SUMMARY OF THE INVENTION

A base portion of an electronic apparatus and a plurality of eligible smart interchangeable covers are provided with corresponding plurality of instructions for the base portion to authenticate a smart interchangeable cover attached to the base portion at power on or reset, or at any other appropriate point in time, as determined by the base portion or the smart interchangeable cover. The base portion operates the electronic apparatus at a function or feature level in view of whether the base portion is able to authenticate the attached smart interchangeable cover or not, selectively enabling/disabling functions/features of the base portion and the attached smart interchangeable cover.

In one embodiment, the base portion would accept data from the smart interchangeable cover (e.g. to personalize or enhance the functions/features of the electronic apparatus), only if the smart interchangeable cover has been authenticated.

In one embodiment, the base portion would operate with at least one of the functions/features offered by the based portion and the smart interchangeable cover at least partially disabled or degraded if the base portion was not able to authenticate the smart interchangeable cover.

In one embodiment, the base portion authenticates the attached cover by challenging the attached cover with one or more challenges, and verifying that the attached cover is able to respond to the one or more challenges with proper responses. In one embodiment, the challenges and responses are exchanged over a secured communication sessions using a set of one or more session keys (SK).

In one embodiment, the set of one or more SKs are generated by the base portion and provided to the attached cover. In one embodiment, the SKs are

provided to the attached cover in an encrypted form, using a public key of the attached cover (CvrKpu). In one embodiment, CvrKpu is provided to the base portion in a signed form using a private signing key (CertSignKpr) of the certification authority and by ways of a certificate signed by a certification authority using a private master key (CertMstrKpr) of the certification authority, and the base portion extracts CvrKpu using a corresponding public signing key (CertSignKpu) of the certification authority, as well as verifying the certificate using a corresponding public master key of the certification authority (CertMstrKpu).

In one embodiment, the subsequent challenges are dependent on the predecessor challenges. In one embodiment, the challenges and responses involve the implementing instructions/data of the functions/features of the attached cover. In one embodiment, the first challenge includes having the attached cover provides the base portion with a manifest enumerating implementing instructions/data of the functions/features of the attached cover, and a signature of the manifest signed by the certification authority, and the second challenge includes having the attached cover provides the base portion with at least one of the functions/features enumerated in the manifest.

In one embodiment, the certification authority is a common licensor, licensing respective manufacturing rights to the vendors of the base portion and attached cover. In one embodiment, the certification authority may revoke previously signed public keys of "once eligible" smart covers, by revoking previously published public signing keys.

In one embodiment, the base portion may employ the assistance of a remote server in authenticating an attached cover. In one embodiment, the base portion may temporarily consider the attached cover as being temporarily authenticated,

until it receives the determination or information contributing to the determination from the assisting remote server.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates an overview of the present invention, in accordance with one embodiment;

Figure 2 illustrates an internal component view of the base portion of the electronic apparatus of **Fig. 1**, in accordance with one embodiment;

Figure 3 illustrates an internal component view of the interchangeable cover of **Fig. 1**, in accordance with one embodiment;

Figure 4 illustrates the operational flow of the relevant aspects of the authentication logic of the base portion of the electronic apparatus of **Fig. 1**, in accordance with one embodiment;

Figure 5 illustrates the operational flow of the relevant aspects of the authentication logic of the interchangeable cover of **Fig. 1**, in accordance with one embodiment;

Figure 6 illustrates one example application of the present invention to wireless mobile phones; and

Figure 7 illustrates another example application of the present invention to personal digital assistants.

DETAILED DESCRIPTION OF THE INVENTION

The present invention includes complementary authentication logics advantageously endowed to the base portion of an electronic apparatus and to their eligible interchangeable covers, to enable the base portion to authenticate an attached cover, to prevent counterfeit covers from being attached to the electronic apparatus.

In the following description, various aspects of the present invention will be described. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, the present invention may be practiced with only some of the described aspects, and without the specific details. In other instances, well-known features are omitted or simplified in order not to obscure the present invention.

The phrase "in one embodiment" will be used repeatedly, however the phrase does not necessarily refer to the same embodiment, although it may. Further, the terms "comprising", "having", "including" and the like are synonymous.

Overview

Referring now to **Figure 1**, wherein a block diagram illustrating an overview of the present invention, in accordance with one embodiment, is shown. As illustrated, base portion **102** of electronic apparatus **100** and eligible smart interchangeable cover **104** are endowed with authentication logic **106** and **108** respectively, to cooperate with each other to effectuate the desired authentication and avoidance of counterfeit covers. For the illustrated embodiment, upon detecting the initial presence of smart cover **104** (at e.g. power on or reset or any arbitrary point in time

selected by either base portion **102** or smart cover **104**), authentication logic **106** of base portion **102** is given execution control, which in turn prompts smart cover **104** for certain information and challenges smart cover **104** to authenticate smart cover **104**. Thereafter, base portion **102** operates electronic apparatus **100** with smart cover **104** attached at a function/feature level consistent with whether base portion **102** is able to authenticate the attached smart cover **104**.

In one embodiment, if authentication logic **106** is able to successfully authenticate smart cover **104**, base portion **102** proceeds to operate apparatus **100**, enabling all the functions and features base portion **102** and smart cover **104** have to offer, less function and features loaded into base portion **102** that are to be enabled only with the presence of particular covers. However, if authentication logic **106** is unable to successfully authenticate smart cover **104**, base portion **102** proceeds to operate apparatus **100**, disabling at least partially one of the functions/features base portion **102** and smart cover **104** have to offer.

In one embodiment, base portion **102** would request **122** and accept the data **124** of smart cover **104** (for personalizing and/or enhancing the functions/features of apparatus **100**) only if it is able to authenticate smart cover **104**. In another embodiment, base portion **102** would request **122** and accept the data **124** of smart cover **104**, even if base portion **102** fails to authenticate smart cover **104**. However, base portion **102** would not fully enable or not enable at all the functions/features implemented by the accepted data **124**. In yet other embodiment, in addition to or in lieu of the aforementioned remedial actions, and disabling functions/features that require presence of certain covers, base portion **102** further partially or fully disable one or more of its own functions/features, if it fails to authenticate attached smart cover **104**, e.g. in the case of a wireless mobile phone application, disabling all

functions, except for the ability to place an emergency call, or a call to the service center of a carrier.

As will be described in more detail below, in one embodiment, authentication logic **106**, authenticates cover **104**, with the cooperation of authentication logic **108**, involving one or more challenges **118** and responses **120** between base portion **102** and cover **104**. In one embodiment, the challenges **118** and responses **120** are exchanged over a secured communication session, using a set of one or more session keys (SK) generated by authentication logic **106**.

In one embodiment, the SKs are provided to authentication logic **108** in an encrypted form **116**, employing a public key (CvrKpu) of cover **104**, which has a corresponding private key (CvrKpr). In one embodiment, the public key CvrKpu of cover **104** is provided to authentication logic **106** in a signed form using a private signing key (CertSignKpr) of a certification authority, and via a certificate **114** signed by the certification authority using its private master key (CertMstrKpr).

In one embodiment, successor challenges are dependent on predecessor responses. In one embodiment, the challenges and responses involve at least a subset of the implementing instructions/data of the functions/features of attached smart cover **104**. In one embodiment, the first challenge includes having authentication logic **108** provides authentication logic **106** a manifest enumerating the implementing instructions/data of the functions/features of attached smart cover **104**, and their corresponding hash values, and a signature of the manifest. In one embodiment, the signature of the manifest is generated by a certification authority.

In one embodiment, the certification authority is the common licensor, licensing respective manufacturing rights to vendors of base portion **102** and eligible smart covers **104**. In one embodiment, the certification authority may revoke previously signed CvrKpus of "once eligible" smart covers **104** by revoking

previously published public signing keys, thereby expiring "once eligible" smart covers **104**. In one embodiment, authentication logic **106** may be assisted by a remote server (if base portion **102** is equipped with appropriate communication capability). In one embodiment where authentication logic **106** is assisted by a remote server, authentication logic **106** may temporarily consider smart cover **104** to be authenticated, until it receives the determination or information contributing to the determination from the assisting remote server.

Except for the respective endowment of authentication logic **106** and **108** to base portion **102** and eligible covers **104**, electronic apparatus **100** may be any one of a wide range of electronic apparatuses, in particular, personal electronic apparatuses, that are amenable to personalization and/or field upgrade of the base portions or base units' functions or features. These electronic apparatuses include but are not limited to pagers, personal digital assistants, wireless mobile phones, game consoles, and so forth.

Personalizing and/or enhancing the functions/features of a base electronic apparatus through smart interchangeable covers is the subject matter of the earlier identified U.S. Provisional Application '326. The specification of which is hereby fully incorporated by reference.

As noted in the incorporated by reference application, the term "wireless mobile phone" as used (in the specification and in the claims) refers to the class or classes of telephone devices (both analog and digital) equipped to enable a user to make and receive calls wirelessly, notwithstanding the user's movement, as long as the user is within the "covered or service area", i.e. within the communication reach of a service or base station of a wireless network. The scope of the "covered or service area" and the signaling protocol are both service provider dependent.

Method of Operation

Still referring to **Fig. 1**, a method of operation of the present invention in accordance with one embodiment, is illustrated. As shown, upon given execution control in response to the detection of the presence or removable attachment of smart cover **104**, during power on or reset (or any arbitrary point in time, selected by either base portion **102** or attached smart cover **104**), for the embodiment, authentication logic **106** of base portion **102** requests smart cover **104** to supply one or more public keys (CvrKpu) of smart cover **104**. In response, authentication logic **108** of authentic smart cover **104** provides the CvrKpu or CvrKpus as requested.

In one embodiment, one CvrKpu is provided, for use by authentication logic **106** to provide SK/Sks to smart cover **104** as well as for use by authentication logic **106** to verify one or more signatures associated with the responses of authentication logic **108** to challenges posed by authentication logic **104**. In one embodiment, at least two CvrKpus are provided, with one CvrKpu for use by authentication logic **106** to provide SK/SKs to smart cover **104**, and another CvrKpu for use by authentication logic **106** to verify one or more signatures associated with the responses of authentication logic **108** to challenges posed by authentication logic **104**.

In one embodiment, authentication logic **108** of smart cover **104** provides the CvrKpu or CvrKpus by way of one or more certificates signed by a certification authority. In one embodiment, each CvrKpu is signed by a private signing key of the certification authority (CertSignKpr), and each certificate is in turn signed by a private master key of the certification authority (CertMstrKpr).

As described earlier, in one embodiment, the authentication authority is a common licensor, licensing respective manufacturing rights to vendors of base portion **102** of the electronic apparatus and eligible smart interchangeable covers **104**.

Authentication logic **106** of base portion **102**, upon receipt of each certificate, extracts the CvrKpu from the received certificate, using a corresponding public signing key of the certification authority (CertSignKpu), which is pre-provided to authentication logic **106**. For the embodiment, authentication logic **106** further authenticates the received certificate, using a corresponding public master key of the certification authority (CertMstrKpu), which is also pre-provided to authentication logic **106**. Recovery of CvrKpu and authentication of the received certificate are dependent on the actual encryption technique employed, which may be any one of a number of techniques known in the art. In one embodiment, the encryption technique employed is the RSA technique.

The key length is dependent on the robustness desired as well as storage capacity of smart cover **104** and/or base portion **102**. In one embodiment, keys of 1024-bit key lengths are employed.

As alluded to earlier, in various embodiments, where base portion **102** is endowed with communication capability, base portion **102** may be provided with revocation information revoking a previously issued public signing key of the certification authority. Thus, even though authentication logic **106** is able to authenticate the certificate, for whatever operational reasons, authentication logic **106** may be prevented from being able to recover CvrKpu(s) of the attached smart cover **104**. Accordingly, authentication logic **106** may be prevented from successfully completing the authentication process, and authenticating a "once eligible", but now "expired" smart cover **104**.

Upon authenticating the received certificate(s), for the embodiment, authentication logic **106** of base portion **102** generates a set of one or more session keys (SKs) for authentication logic **108** of smart cover **104** to be employed for all subsequent authentication related communications. Authentication logic **106** of

base portion **102** encrypts the generated set of one or more SKs using the provided CvrKpu (or an appropriate one of the provided CvrKpus), and provides the SKs to authentication logic **108** of smart cover **104** in an encrypted form.

Authentication logic **108** of smart cover **104**, upon receipt of the encrypted SKs, decrypts and recovers the SKs, using a corresponding private key CvrKpr.

In one embodiment, the 3DES encryption technique is employed to facilitate the exchanges of challenges and responses between authentication logics **106** and **108**. For the embodiment, the set of one or more Sks includes at least 3 session keys. In alternate embodiment, more or less SKs as well as other symmetric or non-symmetric encryption techniques may be practiced instead.

Thereafter, for the embodiment, authentication logic **106** generates a first challenge for authentication logic **108**. The first challenge is provided to authentication logic **108** in encrypted form using the previously provided SKs, thereby increasing the difficulties or burden in the manufacturing of any counterfeit or ineligible smart covers **104**. As alluded to earlier, in one embodiment, the challenges involve implementing instructions/data of functions/features of attached smart cover **104**. More specifically, the first challenge includes having authentication logic **108** provides authentication logic **106** with a manifest enumerating the implementing instructions/data of the functions/features of smart cover **104** and their corresponding hash values, and a signature of the manifest generated by the certification authority.

Then, authentication logic **108** of smart cover **104** provides a response to the challenge (generating the response if necessary). For the embodiment, authentication logic **108** of smart cover **104** provides the response to authentication logic **106** of base portion **102** in an encrypted form, encrypting the response using the provided session SKs.

Upon receipt of the encrypted response, authentication logic **106** of base portion **102** decrypts and recovers the response, using the SKs. Upon recovering the response, authentication logic **106** of base portion **102** determines the "correctness" of response. For the embodiment, authentication logic **106** verifies the manifest using the provided CvrKpu of smart cover **104** or an appropriate one of the provided CvrKpus of smart cover **104**. That is, authentication logic **106** independently generates a hash value for the plaintext of the provided manifest, recovers the reference hash value from a signed hash value provided with the manifest, using the provided CvrKpu, and compares the two hash values.

For the embodiment, as alluded to earlier, subsequent challenges are dependent on predecessor responses. More specifically, upon verifying the signature of the manifest, authentication logic **106** poses another challenge to authentication logic **108**, again in an encrypted form, using the generated SKs. For the embodiment, the second challenge includes having authentication logic **108** provides one or more of the enumerated implementing instructions/data of the functions/features of smart cover **104**. In one embodiment, authentication logic **106** selects which enumerating implementing instructions/data to request in a random manner, to increase unpredictability.

In like manner, authentication logic **108** provides the requested one or more implementing instructions/data in encrypted form, using the provided SKs. Authentication logic **106**, upon recovering the provided instructions/data, in turn independently generates a check hash value for each of the provided implementing instructions/data, and compares each of the generated check hash value to the corresponding hash value earlier provided as part of the signed manifest, to determine whether authentication logic **108** properly responded to the challenge(s).

In various embodiments, authentication logic **106** of base portion **102** may repeat the above described challenge and response process a number of times to satisfy itself that attached smart cover **104** is an eligible or authentic smart cover. The number of repetitions may be fixed or variable, guided by a number of heuristic or other factors.

Upon being satisfied with the authenticity of attached smart cover **104**, base portion **102** signals attached smart cover **104** that it is ready to accept data from smart cover **104**. In response, smart cover **104** provides base portion **102** with its embedded data (to personalize or enhance the functions/features of apparatus **100**).

In various embodiments where base portion **102** is equipped with appropriate communication capabilities, authentication logic **106** may enlist one or more remote servers to assist in authenticating attached smart cover **104**. For some or all of these embodiments, authentication logic **106** may further temporarily assume attached smart cover **104** as being authenticated and operate base portion **102** and attached smart cover **104** accordingly, until it receives the determination or the information to assist authentication logic **106** to make the determination from the assisting remote server or servers.

Base Portion

Figure 2 illustrates a component view of base portion **102** of electronic apparatus **100**, in accordance with one embodiment. As illustrated, apparatus **100** includes elements found in conventional mobile client devices, such as micro-controller/processor **202**, non-volatile memory **204**, and general purpose input/output (GPIO) interface **206**, coupled to each other via bus **208**. In one embodiment, apparatus **100** is a wireless mobile phone, including also elements

such as digital signal processor (DSP), transmit/receive (TX/RX) **312**, and so forth (not shown).

GPIO **206** is used to attach a number of I/O devices to apparatus **100**, including in particular smart cover **104**. Non-volatile memory **204** is used to store programming instructions and data, including in particular, authentication logic **106** and any data (to personalize or enhance the functions/features of apparatus **100**) accepted from smart cover **104**. Except for these uses, the elements are used to perform their conventional functions known in the art, e.g. processor **202** for executing instructions. In the case of a wireless mobile phone, the included DSP and TX/RX are employed to send and receive as well as processing signals, in support of one or more of the known signaling protocols, including but are not limited to CDMA, TDMA, GSM, and so forth. The constitutions of these elements are known. Accordingly, the elements will not be further described.

Smart Cover

Figure 3 illustrates a component view of smart interchangeable cover**104** of electronic apparatus **100**, in accordance with one embodiment. As illustrated, for the embodiment, smart cover **104** includes micro-controller/processor **302** non-volatile storage **304**, and interface **306**, coupled to each other. Micro-controller/processor **302** performs its conventional functions known in the art. Non-volatile storage **304** is used to host authentication logic **108** and data **308** for personalizing or enhancing the functions/features of apparatus **100**. Non-volatile storage **304** may be EEPROM, flash, memory or combinations thereof. In one embodiment, inteface **306** is in the form of a number of contact pins forming a serial or a parallel interface. In one embodiment, one of the contact pins is used to supply power to components **302-306**

of smart cover **104**. In alternate embodiment, other types of interfaces may be used instead.

Operation Flow of Base Portion Authentication Logic

Figure 4 illustrates the operational flow of the relevant aspects of authentication logic **106** of **Fig. 1**, in accordance with one embodiment. As illustrated and alluded to earlier, upon given execution control, authentication logic **106** requests for a public key CvrKpu, block **402**. Thereafter, authentication logic **106** waits for the response of smart cover **104**. After a certain period of time has passed without a response from attached smart cover **104**, authentication logic **106** may determine an authentication error has occurred, and discontinue waiting, in which case smart cover **104** is considered ineligible.

Eventually, authentication logic **106** receives the response. For the embodiment, it is assumed that if smart cover **104** is an eligible smart cover, the response will be in the form of a certificate signed by an authentication authority (which in one embodiment is their common licensor) with the requested CvrKpu being embedded therein. Accordingly, upon receipt of the certificate, authentication logic **106** extracts CvrKpu using CertSIgnKpu, block **404**. For the embodiment, as alluded to earlier, authentication logic **106** further verifies the certificate using CertMstrKpu.

Assuming the certificate is verified, authentication logic **106** generates a set of SKs to facilitate subsequent exchanges of challenges and responses between authentication logics **106** and **108**, encrypts the SKs using the provide CvrKpu or an appropriate provided one of the CvrKpus, and provides the SKs in an encrypted form to authentication logic **108**, block **405**.

Then, authentication logic **106** provides a challenge, encrypting the challenge using the provided CvrKpu or an appropriate one of the provided CvrKpus, and

transmits the encrypted challenge to smart cover **104**, block **406**. Thereafter, authentication logic **106** again waits for the response of smart cover **104**.

Eventually, authentication logic **106** receives the response to the challenge it posed. For the embodiment, the response to the challenge is returned in an encrypted form using the provided SKs. Accordingly, upon receipt of the encrypted response to the challenge, authentication logic **106** recovers the response, decrypting the encrypted response using the generated Sks, and then verifies the recovered response, block **408**. In one embodiment, as described earlier, verification includes verifying the signature of a manifest of smart cover **104** for a first response to a first challenge using CvrKpu, and verifying hash values of implementing instructions/data of smart cover **104** for later responses to subsequent challenges.

At block **410**, authentication logic **106** determines whether smart cover **104** has successfully responded to sufficiently number of challenges to be considered as an eligible cover.

Eventually, smart cover **104** has either successfully responded to a sufficient number of challenges to be considered as an eligible cover, or has failed to respond to a point that the smart cover is to be considered as ineligible. At such time, authentication logic **106** generates an indication for base portion **102** denoting whether attached smart cover **104** is to be considered as an eligible or ineligible cover, block **412**.

Thereafter, as described earlier, in one embodiment, base portion **102** proceeds to request smart cover **104** for its data (to personalize or enhance the functions/features of apparatus **100**), if the indication generated by authentication logic **104** denotes that smart cover **104** is an eligible cover. In one embodiment, base portion **102** simply ignores the attached smart cover **104** if the indication generated by authentication logic **104** denotes that smart cover **104** is an ineligible cover.

Operation Flow of Base Portion Authentication Logic

Figure 5 illustrates the operational flow of the relevant aspects of authentication logic **108** of **Fig. 1**, in accordance with one embodiment. As illustrated, for the embodiment, upon receipt of a request for a CvrKpu from base portion **102** to which smart cover **104** is attached, authentication logic **108** provides authentication logic **106** of base portion **102** a CvrKpu corresponding to its CvrKpr (in a signed form and by way of a signed certificate), block **501**. Next, for the embodiment, authentication logic **108** receives a set of SKs from authentication logic **106**, to facilitate subsequent exchanges of challenges and responses between authentication logics **106** and **108**, block **502**. Thereafter, authentication logic **108** waits for a challenge from authentication logic **104** of base portion **102**.

Eventually, authentication logic **108** receives the challenge encrypted using the SKs, as described earlier. In response, authentication logic **108** decrypts the encrypted challenge using the provided SKs, block **504**. Upon recovering the challenge, authentication logic **108** provides a response to the challenge (generating it if necessary). For the embodiment, authentication logic **108** encrypts the response using the SKs, and provides the encrypted response as its reply to the challenge posted by authentication logic **106**, block **506**. Thereafter, authentication logic **108** waits for another challenge from authentication logic **104** of base portion **102**.

Assuming eventually, authentication logic **104** is satisfied that attached smart cover **104** is an eligible cover, and ceases to pose further challenges.

As described earlier, in one embodiment, base portion **102** then proceeds to request for the implementing instructions/data of the functions/features of smart cover **104** (to personalize or enhance the functions/features of apparatus **100**). In

response, smart cover **104** provides its functions/features' implementing instructions/data as requested.

Example Applications

Figures 6a-6b illustrate an example application of the present invention to a wireless mobile phone, in accordance with one embodiment. Shown in **FIG. 6a** is an exposed view of wireless mobile phone **600**, without its cover, exposing its base portion **602**. Shown in **FIG. 6b** is a complementary smart interchangeable cover **620**, designed for attachment to, and covering base portion **602** of wireless mobile phone **600**. Further, smart interchangeable cover **620** comprises implementing instructions/data to personalize and/or enhance the functionalities of wireless mobile phone **600**.

The orientation of the illustrations in **Fig. 6a-6b** is that the right side of base portion **602** corresponds to (or engages with) the left side of smart interchangeable cover **620**, and the left side of base portion **602** corresponds to (or engages with) the right side of the interchangeable covering **620**.

Base portion **602** includes contacts **604** that are pressed by a keypad **625** formed with keys **621** molded onto smart interchangeable cover **620**. Additionally, the base portion also includes a display, such as, a liquid crystal display (LCD) **607**, a microphone **608**, and a speaker **609**. LCD **607** corresponds to a transparent area or cutout **616** to facilitate exposure of a graphical user interface. Speaker **609** and microphone **608** correspond to the audio transmissive area for sound transmission **624**, and the audio transmissive area for sound reception **623**, respectively on smart interchangeable cover **620**, for audio transmission and receipt.

Smart interchangeable cover **620** includes electronic component **623** having the earlier described data and/or programming instructions for personalizing or

enhancing the functionalities of wireless mobile phone **600**. Electronic component **623** includes contacts **622** designed to mate with contacts **611** of base portion **602**.

In one embodiment, the data and/or programming instructions provide a customized ring tone complementary to an aspect of a personalizing theme conveyed by the design and color of cover **620**. Additionally, the data and/or programming instructions include address specifications designating locations on a network where additional data and/or programming instructions for further personalizing or enhancing the functionalities may be retrieved. The address specifications may be in the form of one or more Uniform Resource Locators (URLs).

From hereon forward (including the claims), for ease of understanding, "data and/or programming instructions" will simply be referred to as "data". Usage of the term "data" includes "data" as it is conventionally used, and/or "programming instructions", unless the implicit optional inclusion of "programming instructions" is explicitly excluded.

Smart interchangeable covering **620** in **Fig. 6b** is shown as substantially similar in shape, length, and width to wireless mobile phone **600**. However, smart interchangeable covering **620** may be of any shape and size to cover all or portions of wireless mobile phone **600**, such as, but not limited to, an interchangeable covering that covers only a portion of the wireless mobile phone **600**. Smart interchangeable cover **620** may cover only the face of wireless mobile phone **600**. Additionally or alternatively, it may cover the sides of wireless mobile phone **600** or portions thereof. Smart interchangeable cover **620** may also cover the back of wireless mobile phone **600** or portions thereof.

Figures 7a-7b illustrate another example application of the present invention to a personal digital assistant, in accordance with one embodiment. Shown in **Figs. 7a-7b**, is a personal digital assistant (PDA) **700** (also referred to as handheld personal computer or handheld PC) with its cover removed, and a complementary smart interchangeable cover **710**.

Similar to the earlier described wireless mobile phone application, base portion **702** of PDA **700** includes various buttons **704** and **705** for activating certain functions, such as, but not limited to, scrolling through displayed information, LCD **706** to display the information and form a graphical interface, and, optionally, antenna **703** to receive and transmit data from the exposed PDA **700**. Shown also, disposed on smart interchangeable covering **720**, are various openings **725** to allow the various buttons **704** and **705** to be pressed through interchangeable PDA cover **720**.

Smart interchangeable cover **720** also includes electronic component **723** having the earlier described data and/or programming instructions for personalizing or enhancing the functionalities of PDA **700**. Electronic component **723** also includes contacts **727** designed to mate with contacts **711** of base portion **702**.

More importantly, as the earlier described wireless mobile phone application, both the base portion and the cover are endowed with the complementary authentication logics of the present invention for the base portion to authenticate the cover, before accepting personalizing and/or function enhancing data from the cover.

Conclusion and Epilogue

Thus, a method and apparatus for avoiding counterfeit attachment of a smart interchangeable cover to a base portion of an electronic apparatus has been

described. While the present invention has been described in terms of the above-illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims. For examples, the specific encryption/decryption technique used in a specific stage of the authentication process, and the kind, the number as well as the length of keys used may also vary from embodiments to embodiments. Likewise, the nature of challenges and responses, and the resulting operational states of the apparatus may all vary from embodiments to embodiments. Thus, the description is to be regarded as illustrative instead of restrictive on the present invention.